IN THE CLAIMS:

Claims 6 - 11, 20, 28, 31, 37, and 38 have been amended. Claims 1 - 3 have been cancelled. Claims 42 - 52 have been added.

Claims 1 - 5. (cancelled)

6. (currently amended) The computer network of claim [[1]] 31, further including logic for allowing the traffic communication between the server system and the client system to be sent without security.

7. (currently amended) The computer network of claim [[1]] 31, wherein the client system is a network device.

8. (currently amended) The computer network of claim [[1]] 31, wherein the storage device is at least one of an Ethernet device, a coprocessor connected to an Ethernet device, and non-volatile storage that is part of an Ethernet device.

9. (currently amended) The computer network of claim [[1]] 31, wherein the logic for inhibiting the stored results of the first key exchange process from being updated includes:

logic for sending a signal acknowledging the successful execution of another set of key exchange processes; and

logic for sending a signal confirming receipt of the acknowledgement signal.

10. (currently amended) The computer network of claim [[1]] 31, wherein the server system contains a storage device for storing the results of the first key exchange ~~processes~~ process and the second key exchange process.

11. (currently amended) The computer network of claim [[1]] 31, further comprising logic for switching the server system to a second server system in the

computer network if the server system becomes non-operational, security mechanisms securing traffic communication between the second server system and the client system.

Claims 12 - 19 (cancelled).

20. (currently amended) A method of providing security mechanisms for securing traffic communication between a server system and a client system, the method comprising:

detecting whether the client system is in an operational state;

executing first key exchange processes between the server system and the client system if the client system is in the operational state;

storing the results of the first key exchange processes into the client system;

inhibiting the stored results from being updated until a successful execution of second key exchange processes between the server system and the client system;

and using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes are not successful because the client system becomes non-operational, wherein the results of the first key exchange process are utilized even if a security parameter refresh timer has elapsed and no acknowledgment signal is received.

Claims 21 and 22 (cancelled).

23. (previously presented) The method of claim 20, further including allowing the traffic communication between the server system and the client system to be sent without security.

24. (previously presented) The method of claim 20, wherein the results of the

first key exchange processes and the second key exchange processes are stored into at least one of a network device, a coprocessor connected to a network device, and non-volatile storage that is part of a network device.

25. (previously presented) The method of claim 20, wherein inhibiting the stored results of the first key exchange processes from being updated includes:

sending a signal acknowledging the successful execution of the second key exchange processes; and

sending a signal confirming receipt of the acknowledgement signal.

26. (previously presented) The method of claim 20, further including storing the results of the first key exchange processes and the second key exchange processes into the server system.

27. (previously presented) The method of claim 20, further including switching the server system to a second server system in the computer network if the server system becomes non-operational, the security mechanisms securing traffic communication between the second server system and the client system.

28. (currently amended) ~~The method of claim 20,~~ A method of providing security mechanisms for securing traffic communication between a server system and a client system, the method comprising:

detecting whether the client system is in an operational state;

executing first key exchange processes between the server system and the client system if the client system is in the operational state;

storing the results of the first key exchange processes into the client system;

inhibiting the stored results from being updated until a successful execution of a

second key exchange processes between the server system and the client system; and

using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes are not successful if because the client system becomes non-operational, wherein using the stored results to secure the traffic communication further includes transmitting management Internet Protocol-based packets from the server system to the client system, if the client system is determined to be non-operational, to perform diagnostic operations on the client system.

29. (previously presented) The method of claim 28, wherein the transmission of management IP-based protocol packets causes the client system to re-boot.

30. (previously presented) The method of claim 29, wherein the management IP-based protocol packets are remote management and control protocol (RCMP) packets.

31. (currently amended) ~~The network system of claim 1,~~ A computer network comprising:

a server system;

a client system;

logic for detecting whether the client system is in an operational state;

logic for executing a first key exchange process between the server system and the client system to produce results;

a storage device at the client system for storing the results of the first key exchange process;

logic for inhibiting the stored results of the first key exchange process from being updated until a successful execution of a second key exchange process between the

server system and the client system;

logic for updating the stored results of the first key exchange process if the execution of the second key exchange process is successful;

logic to secure traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-operational, and

~~further including~~ a plurality of client systems including the client system coupled to the server system, each of the plurality of client systems including a security parameter, wherein the server system includes a non-volatile storage for storing the security parameter for each of the plurality of client systems.

32. (currently amended) A client system, comprising:

logic for executing a first key exchange process between a server and the client system to product results;

a storage device to store the results of the first key exchange process;

logic for inhibiting the stored results of the first key exchange process from being updated until a second key exchange process is successful;

logic for updating the stored results of the first key exchange process if execution of second key exchange process is successful; and

logic to secure the traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-operational, wherein the results of the first key exchange process are utilized even if a

security parameter refresh timer has elapsed and no acknowledgment signal is received.

33. (previously presented) The client system of claim 32, further including logic for allowing the traffic communication between the server system and the client system to be sent without security.

Claim 34. (cancelled)

35. (previously presented) The client system of claim 32, wherein the client system is a network device.

36. (previously presented) The client system of claim 32, wherein the storage device is at least one of an Ethernet device, a coprocessor connected to the Ethernet device, and a non-volatile storage that is part of the Ethernet device.

37. (currently amended) ~~The client system of claim 32,~~ A client system, comprising:

logic for executing a first key exchange process between a server and the client system to product results;

a storage device to store the results of the first key exchange process;

logic for inhibiting the stored results of the first key exchange process from being updated until a second key exchange process is successful;

logic for updating the stored results of the first key exchange process if execution of second key exchange process is successful; and

logic to secure the traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-

operational, wherein the securing of the communication traffic further includes logic for receiving management Internet Protocol-based packets from the server system if the client system is determined to be non-operational to perform diagnostic operations on the client system.

38. (currently amended) A computer readable medium, the computer readable medium including computer readable instructions encoded thereon, which when executed cause a client system to:

execute a first key exchange process between a server system and the client system if the client system is in an operational state;

store results of the first key exchange process in the client system;

inhibit the stored results from being updated until a successful execution of a second key exchange process between the server system and the client system; and

use the stored results of the first key exchange process to secure the traffic communication if the second key exchange process is not successful because the client system is non-operational even if a security parameter refresh timer has elapsed and an acknowledgment message is not received at the client system.

39. (previously presented) The computer readable medium of claim 38, further including computer readable instructions encoded thereon, which when executed cause the client system to allow the traffic communication between the server system and the client system to be sent without security.

40. (previously presented) The computer readable medium of claim 38, wherein the instructions to inhibit the stored results of the first key exchange process from being updated include sending a signal acknowledging the successful execution of the

second key exchange process; and

sending a signal confirming receipt of the acknowledgment signal.

41. (previously presented) The computer readable medium of claim 38, further including computer readable instructions encoded thereon, which when executed cause the client system to switch the server system to a second server system in the computer network if the server system becomes non-operational, where the second server system includes security mechanisms for securing traffic communication between the second server system and the client system.

42. (new) A method of providing security mechanisms for securing traffic communication between a server system and a client system, the method comprising:

detecting, at the client system, whether the client system is in an operational state;

initiating first key exchange processes, from the client system, between the server system and the client system if the client system is in the operational state;

storing the results of the first key exchange processes in the client system;

inhibiting the stored results from being updated in the client system until a successful execution of a second key exchange processes between the server system and the client system; and

using the stored results of the first key exchange processes to secure the traffic communication if the second key exchange processes are not successful if the client system becomes non-operational, wherein using the stored results to secure the traffic communication further includes receiving management Internet Protocol-based packets from the server system at the client system, if the client system is determined to be

non-operational, to perform diagnostic operations on the client system.

43. (new) The method of claim 42, wherein the traffic communication between the server system and the client system is sent without security.

44. (new) The method of claim 42, further including switching communications to a second server system if the server becomes non-operational.

45. (new) A computer readable medium, the computer readable medium including computer readable instructions encoded thereon, which when executed cause a client system to:

execute a first key exchange process between a server and the client system to product results;

store results of the first key exchange process in a storage device;

inhibit the stored results of the first key exchange process from being updated until a second key exchange process is successful;

updating the stored results of the first key exchange process if execution of second key exchange process is successful; and

securing the traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-operational, wherein using the stored results to secure the traffic communication further includes receiving management Internet Protocol-based packets from the server system at the client system, if the client system is determined to be non-operational, to perform diagnostic operations on the client system.

46. (new) The computer-readable medium of claim 45, wherein the traffic

communication between the server system and the client system is sent without security.

47. (new) The computer-readable medium of claim 45, which when executed cause the client system, to further include switching communications to a second server system if the server becomes non-operational.

48. (new) A method, comprising:

determining whether a client system is in an operational state;

initiating a first key exchange process, at a server system, between the server system and the client system to produce results;

storing the results, at the server system, of the first key exchange process;

inhibiting the stored results of the first key exchange process from being updated until a successful execution of a second key exchange process between the server system and the client system;

updating the stored results of the first key exchange process at the server system if the execution of the second key exchange process is successful;

securing traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-operational; and

storing a security parameter for each of a plurality of client systems in a non-volatile storage, wherein each of the plurality of client systems, which are all coupled to the server, have a corresponding security parameter.

49. (new) The method of claim 48, wherein the traffic communication between the server system and the client system is sent without security.

50. (new) The method of claim 48, further including switching communications to a second server system if the server becomes non-operational.

51. (new) A computer readable medium, the computer readable medium including computer readable instructions encoded thereon, which when executed cause a server system to:

determine whether a client system is in an operational state;

initiate a first key exchange process, at the server system, between the server system and the client system to produce results;

store the results, at the server system, of the first key exchange process;

inhibit the stored results of the first key exchange process from being updated until a successful execution of a second key exchange process between the server system and the client system;

update the stored results of the first key exchange process at the server system if the execution of the second key exchange process is successful;

secure traffic communication between the client system and the server system utilizing the results of the first key exchange process if the second key exchange process is not successful because the client system becomes non-operational; and

store a security parameter for each of a plurality of client systems including the client system in a non-volatile storage, wherein each of the plurality of client systems, which are all coupled to the server system, have a corresponding security parameter.

52. (new) A method of securing traffic communications between a client system and a server system, comprising:

executing a first key exchange process between the server system and the client

system if the client system is in an operational state;

storing results of the first key exchange process in the client system;

inhibiting the stored results from being updated until a successful execution of a second key exchange process between the server system and the client system; and

using the stored results of the first key exchange process to secure the traffic communication if the second key exchange process is not successful because the client system becomes non-operational even if a security parameter refresh timer has elapsed and no acknowledgment is received.